PATENT ABSTRACTS OF JAPAN

(11)Publication number : 03-185586
(43)Date of publication of application : 13.08.1991

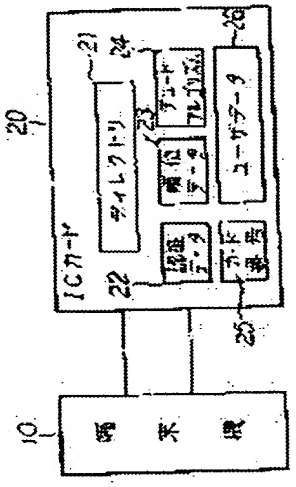
(51)Int.Cl. G06K 17/00
G07F 7/12

(21)Application number : 01-325663
(22)Date of filing : 14.12.1989

(71)Applicant : DAINIPPON PRINTING CO LTD
(72)Inventor : YOSHIDA HIDEYO
WAKAMATSU MASAKI

(54) METHOD FOR CERTIFYING ID CARD

(57)Abstract:
PURPOSE: To improve operability and to secure highly efficient security by updating the registration of priority order from an external terminal equipment.
CONSTITUTION: When a certification(CF) command is applied from the terminal equipment 10, CF data are read out to a CF data area 22 in an ID card 20. Whether the read CF data coincide with the CF data inputted by a user to the terminal equipment 10 in accordance with the priority order indicated by order data in an order data area 23 or not is decided. The registration of the priority order is allowed to be updated from the external terminal equipment. Even if the collating procedure of the ID card is known by a third person, the card is not invalidly accessed by the third person by changing the priority order and its security can be improved. Since the ID card can be accessed by the same collating procedure until the priority order is changed, the operability can be improved.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

3. Japanese Patent Application, Publication No.H03-185586

Lines between ln.10 of upper-right col. and ln.11 of lower-left col. on page 4

The IC card 20 on receiving this general command from the terminal unit 10, first reviews a match flag (Step S8). If the flag-value is 1, indicating the verification command has been executed and an associated matching has resulted to confirm the "matched", the operation flow moves to Step S9. In Step S9, an assigned general command is executed. The process executed with this command may, for example, be of reading out some user data or entering a change into the user data. Then, in Step S10, it is determined if the process has been properly executed and, on confirming it having been proper, the flow moves to Step S11, in which a proper-status indicator is set. Alternatively, if the flag-state is in 0, in Step S8, or if it is found in Step S10 that the process has not been executed properly, a error-status indicator is set in Step S12. As it has been described above, no command is executed in Step S9 until the verification command has been executed and the match flag value is set to 1. This implies that it is impossible for a user to access user data unless the user enters correct pieces of verification data in a correct priority order.

Fig. 1

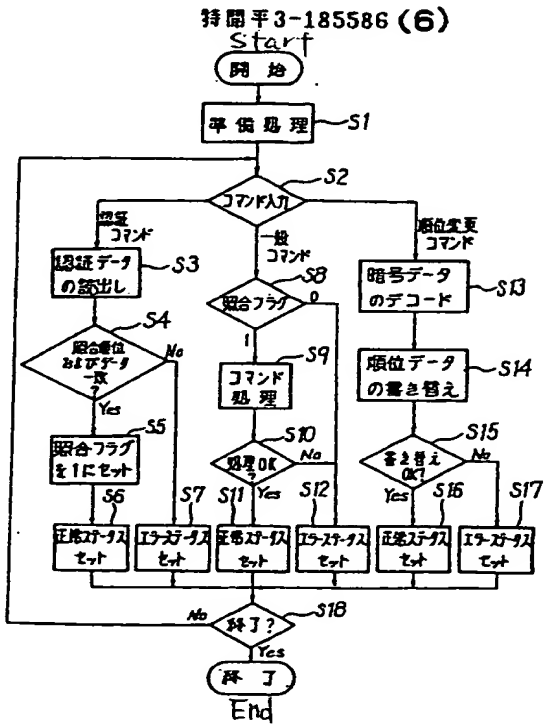
Start
S1: Preparatory process
S2: Command input
If input is a verification command, move to S3
If input is a general command, move to S8
If input is a order change command, move to S13
S3: Reads out pieces of verification data
S4: Is match priority order correct, does data pieces match?
If yes then move to S5.
If no then move to S7
S5: Set match flag value to 1
S6: Indicate proper status and move to S18

S7: Indicate error status and move to S18

S8: Match flag
If it is set to 1, move to S9
If it is set to 0, move to S12
S9: Execute command
S10: Has the process executed properly?
If yes, move to S11
If no, move to S12
S11: Indicate proper status and move to S18
S12: Indicate error status and move to S18

S13: Decode encrypted data and move to S14
S14: Rewrite order specifying data and move to S15
S15: Is it OK to rewrite?
If yes, move to S16
If no, move to S117
S16: Indicate proper status and move to S18
S17: Indicate error status and move to S18

S18: Do you end the process?
If yes, then End
If no, move to S2



⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　平3－185586

⑤Int. Cl.⁵	識別記号	庁内整理番号	⑬公開　平成3年(1991)8月13日
G 06 K 17/00	T	6711－5B	
G 07 F 7/12		8208－3E　G 07 F 7/08　C	

審査請求　未請求　請求項の数 3　（全6頁）

⑭発明の名称　ＩＣカードの認証方法

⑳特　願　平1－325663
㉒出　願　平1(1989)12月14日

㉑発明者　吉田　英世　東京都新宿区榎町7番地　大日本印刷株式会社内
㉑発明者　若松　雅樹　東京都新宿区榎町7番地　大日本印刷株式会社内
㉑出願人　大日本印刷株式会社　東京都新宿区市谷加賀町1丁目1番1号
㉔代理人　弁理士　志村　浩

明　細　書

1．発明の名称

ＩＣカードの認証方法

2．特許請求の範囲

(1)　ＩＣカード内に、複数組の認証データとこの認証データの優先順位とを登録しておき、外部の端末機に用意された複数組の認証データに対して、前記登録した複数組の認証データを前記登録した優先順位で照合するＩＣカードの認証方法において、

外部の端末機から前記優先順位の登録を更新しうるようにしたことを特徴とするＩＣカードの認証方法。

(2)　ＩＣカード内に、複数組の認証データとこの認証データの優先順位とを登録しておき、外部の端末機に用意された複数組の認証データに対して、前記登録した複数組の認証データを前記登録した優先順位で照合するＩＣカードの認証方法において、

ＩＣカード内に、個々のＩＣカードに固有な識別データと、この識別データを利用して暗号データをデコードするアルゴリズムと、を記憶させ、

外部の端末機から暗号データが与えられたときに、前記アルゴリズムに基づいてこの暗号データをデコードし、このデコード結果に基づいて前記優先順位の登録を新たなものに更新することを特徴とするＩＣカードの認証方法。

(3)　請求項2に記載のＩＣカードの認証方法において、

認証データの組数ｎと同じ桁数ｎの暗号データを用い、

識別データを構成する各桁を、ｎ列複数行の行列に配し、各列ごとに論理演算を行いｎ個の値を求め、このｎ個の値のそれぞれと前記暗号データの各桁のそれぞれとの間で論理演算を行い前記ｎ個の値を更新し、このｎ個の更新値の大きさの順に基づいて新たな優先順位を決定することを特徴とするＩＣカードの認証方法。

３．発明の詳細な説明

〔産業上の利用分野〕

本発明はＩＣカードの認証方法、特に、複数組の認証データとこの認証データの優先順位とをＩＣカードに登録しておくＩＣカードの認証方法に関する。

〔従来の技術〕

磁気カードに代わる媒体として、ＩＣカードの普及が期待されているが、ＩＣカードの用途が広がれば広がるほど、セキュリティの重要性が増してくる。このため、ＩＣカードを用いる場合には、その都度、認証を行うシステムが不可欠となる。

通常の認証方法としては、ＩＣカード内の特定のメモリエリアに、認証データを登録しておき、ユーザーが端末機に与えた認証データと、ＩＣカード内に登録された認証データとを比較する方法が行われている。また、更にセキュリティを向上させる方法として、たとえば、特開昭６２－１９０５８３号公報には、ＩＣカード内に、複数組の認証データを登録しておき、この複数組の認証データを種々のケースに応じて種々の優先順位で読出して照合する方法が開示されている。

〔発明が解決しようとする課題〕

上述の複数組の認証データを用いる方法では、単一の認証データを用いる方法に比べてセキュリティはかなり向上することになる。しかしながら、ユーザーは各ケースごとに認証データの入力を異なる順序で行う必要があり、操作性が悪くなるという問題がある。たとえば、前述の公報に実施例として記載された方法では、ＩＣカードをアクセスしたときの時刻に応じて１０とおりの優先順位を定めているが、ユーザーはそのときの時刻によって、認証データの入力順序を変えねばならず、非常に不便である。また、他人に認証手順を知られた場合、その認証手順が有効になる場合が１／１０の確率で発生し、セキュリティの面でも問題がある。

そこで本発明は、操作性が良く、しかも高度なセキュリティを確保することのできるＩＣカードの認証方法を提供することを目的とする。

〔課題を解決するための手段〕

(1)　本願第１の発明は、ＩＣカード内に、複数組の認証データとこの認証データの優先順位とを登録しておき、外部の端末機に用意された複数組の認証データに対して、登録した複数組の認証データを登録した優先順位で照合するＩＣカードの認証方法において、

外部の端末機から優先順位の登録を更新しうるようにしたものである。

(2)　本願第２の発明は、ＩＣカード内に、複数組の認証データとこの認証データの優先順位とを登録しておき、外部の端末機に用意された複数組の認証データに対して、登録した複数組の認証データを登録した優先順位で照合するＩＣカードの認証方法において、

ＩＣカード内に、個々のＩＣカードに固有な識別データと、この識別データを利用して暗号データをデコードするアルゴリズムと、を記憶させ、

外部の端末機から暗号データが与えられたときに、記憶しているアルゴリズムに基づいてこの暗号データをデコードし、このデコード結果に基づいて優先順位の登録を新たなものに更新するようにしたものである。

(3)　本願第３の発明は、上述の第２の発明において、

認証データの組数ｎと同じ桁数ｎの暗号データを用い、

識別データを構成する各桁を、ｎ列複数行の行列に配し、各列ごとに論理演算を行いｎ個の値を求め、このｎ個の値のそれぞれと暗号データの各桁のそれぞれとの間で論理演算を行いｎ個の値を更新し、このｎ個の更新値の大きさの順に基づいて新たな優先順位を決定するようにしたものである。

〔作　用〕

(1)　本願第１の発明によれば、外部の端末機から優先順位の登録を更新することができる。したがって、他人に照合手順を知られたとしても、優先順位を変えてしまえば、もはや他人の不正なアクセスを受けることがなく、セキュリティが向

上する。また優先順位を変更する操作を行わない限り、同じ照合手順でアクセスできるため、操作性も良好である。

(2)　本願第２の発明によれば、優先順位の登録更新操作を行う場合、新たな優先順位を示す順位データは、そのままではなく暗号データの形式で端末機からＩＣカードへと伝えられる。したがって、セキュリティ性がより向上する。

(3)　本願第３の発明によれば、ＩＣカード固有の識別データに基づいて生成された行列と、与えられた暗号データと、に基づいて優先順位が決定される。したがって、セキュリティ性の高い更新作業が可能になる。

〔実施例〕

以下、本発明を図示する実施例に基づいて説明する。第１図は本発明の一実施例に係る認証方法を利用したＩＣカードのアクセス手順を示す流れ図である。この手順について詳述する前に、ＩＣカード内のデータ構成について簡単に説明しておく。第２図は、端末機１０にＩＣカード２０を接続した状態を示すブロック図である。端末機１０とＩＣカード２０との間では、図の矢印に示すようにデータがやりとりされる。ＩＣカード２０内には、種々のデータを格納するため、次の各領域が設けられている。

ディレクトリ領域２１

他の各領域をアクセスするためのアドレス値などのディレクトリ情報が格納される。

認証データ領域２２

複数組の認証データが格納される。ここで説明する例では、第３図に示すような４組の認証データ（いずれも１６進データで示してある）を用いている。

順位データ領域２３

複数組の認証データの優先順位を示す順位データが格納される。各認証データは、この優先順位にしたがって照合されることになる。この例では、前述のように４組の認証データが用いられているので、順位データはこの４組についての照合順位を示すものとなる。第４図は、この順位データの一例を示すものであり、この例によれば、認証データ②④①③の順序で照合が行われることになる。

デコードアルゴリズム領域２４

端末機１０から与えられた暗号データをデコードするためのアルゴリズムが格納される。具体的には、デコードのためのプログラムが格納されることになる。

カード番号領域２５

各ＩＣカードを識別するための固有のデータであるカード番号が格納される。この例では、たとえば、第５図に示すような１８桁（本明細書では、一連のデータを構成する１データ単位を１桁と呼ぶことにする。この例では１バイトのデータ単位を１桁と呼んでいる）のデータからなるカード番号が格納されている。

ユーザデータ領域２６

ＩＣカードが記憶すべき本来のデータであるユーザデータが格納される。

なお、ＩＣカードは、上述の各領域を有するメモリの他に、ＣＰＵなどのプロセッシングユニットを備えているが、第２図には示されていない。

それでは、第１図の流れ図を参照して、この実施例のＩＣカードのアクセス手順を説明する。はじめに、ユーザがＩＣカード用のリーダ／ライタ装置にＩＣカードを挿入すると、ステップＳ１の準備処理が行われる。この準備処理は、端末機１０とＩＣカード２０との間でデータのやりとりを行うための準備を行う処理であり、たとえば、端末機１０からＩＣカード２０に対して RESET信号を与えると、これに応じてＩＣカード２０から端末機１０へ ANSVER TO RESET信号が返されることになる。

準備処理が完了すると、ステップＳ２において端末機１０からＩＣカード２０へのコマンド入力を待つ状態となる。このコマンドは、認証コマンド、一般コマンド、順位変更コマンド、の３種類に分類され、コマンドの種類によってＩＣカード２０内の処理が異なる。

認証コマンドは、このＩＣカードの持ち主が正当なユーザであるか否かを認証する作業を行うた

めのコマンドであり、通常は、ユーザデータをアクセスする前にこのコマンドが実施される。端末機１０からこの認証コマンドが与えられると、ＩＣカード２０内において、ステップＳ３に示すように、認証データ領域２２から認証データの読出しが行われる。読出された認証データは、順位データ領域２３内の順位データに示す優先順位の順にしたがって、ユーザが端末機１０に入力した認証データと一致するかが判定される（ステップＳ４）。この実施例の場合、第３図に示す４組の認証データが読み出され、第４図に示す順位、すなわち、認証データ②④①③の順序で照合が行われることになる。別言すれば、ユーザが端末機１０に対して、認証データ②④①③の順で入力したときにのみ、両者は一致することになる。一致した場合には、ステップＳ５において照合フラグが１にセットされる。この照合フラグは、照合結果が一致した場合に１となり、不一致の場合あるいは認証作業がまだ行われていない場合には０となる。更にステップＳ６において正常ステータスがセットされる。一方、ステップＳ４において不一致であった場合には、ステップＳ７においてエラーステータスがセットされる。したがって、この場合は照合フラグは０のままとなる。以上が認証コマンドに対する処理手順である。

一般コマンドは、このＩＣカードに対する本来のアクセス用コマンドである。たとえば、ユーザデータを端末機１０側に読み出したり、ユーザデータを書き替えたりするコマンドなどが、この一般コマンドとなる。ＩＣカード２０は、端末機１０からこの一般コマンドが与えられると、はじめにステップＳ８において照合フラグのチェックを行う。そして、照合フラグが１であれば、すなわち、既に認証コマンドに対する処理が行われ照合結果が一致した場合には、ステップＳ９へと進む。このステップＳ９では、与えられた一般コマンドに対する処理が行われる。たとえば、ユーザデータの読み出しや書き替えといった処理が実際に行われる。そして、ステップＳ１０においてこの処理が正常に行われたか否かが判断され、正常に行われた場合にはステップＳ１１において正常ステータスがセットされる。また、ステップＳ８において、照合フラグが０であった場合、あるいはステップＳ１０において異常発生と判断された場合には、ステップＳ１２においてエラーステータスがセットされる。このように、認証コマンドを行い、照合フラグが１にセットされない限り、ステップＳ９のコマンド処理を行うことはできない。別言すれば、ユーザが正しい認証データを正しい優先順位で入力しない限り、ユーザデータをアクセスすることはできない。

順位変更コマンドは、本願発明の特徴となる処理を行うためのコマンドである。このコマンドの目的は、順位データ領域２３内の順位データを変更することである。これはたとえば、ユーザが他人に認証データの入力操作を知られてしまったような場合に有効である。順位データを変更してしまえば、他人の知っている入力操作では、認証データの優先順位が異なるため、照合一致が不可能になり、セキュリティを向上させることができる。第４図に示す例では、現在の順位データは「２４１３」である。いま、この順位データを「３４１２」に変更する場合を例として説明する。はじめに、端末機１０から、新たな順位データ「３４１２」に相当する暗号データをＩＣカード２０に与える。この暗号データは、ＩＣカードのカード番号を用いて作成される。暗号の作成手順は、後述する暗号のデコード手順の逆であるから、ここでは説明を省略する。ＩＣカード２０は、暗号データを受け取ると、ステップＳ１３においてこれをデコードする。デコードのためのアルゴリズムは、デコードアルゴリズム領域２４内にプログラムとして記述されている。ここに述べる実施例では、次のようにしてデコードされる。まず、端末機１０側から与えらえた暗号データを、Ｘ１，Ｘ２，Ｘ３，Ｘ４とする。このアルゴリズムでは、暗号データの桁数は認証データの組数に一致する。したがって、この例の場合、４桁の暗号データが作成されている。はじめに、ＩＣカード２０は、自分自身に与えられた固有の識別データであるカー

ド番号を読み出す。ここで説明する例では、第５図に示す１８桁（前述のように、この例では１バイトを１桁と呼ぶ）のカード番号が読み出される。このカード番号は、第６図に示すように、行列に配される。ここで、１行の列数は認証データの組数と一致させるようにする。すなわち、この例の場合は１行は４列で構成され、読み出したカード番号の最初の４桁は１行目、次の４桁は２行目、というように順に並べられてゆく。結局、この例の場合、５行４列の行列が形成されるが、カード番号は１８桁しかないため、５行目の行列要素は２桁分不足する。そこで、これに対してパディング処理を施す。すなわち、不足分を何らかのデータで補うのである。どのようなデータで補うかは、予め決めておくことになるが、この実施例では、不足箇所には常に「２０」なるデータを補うことにしている。こうして、第６図に示すような５行４列の行列が完成すると、各列ごとに論理演算を施す。たとえば、第１列目については、「Ａ０，Ａ４，Ａ８，ＡＣ，Ｂ０」なる５桁のデータに対して何らかの論理演算が施され、演算結果としてＹ１が得られる。この論理演算はどのようなものでもかまわないが、予め決めておかねばならない。たとえば、全データの論理和、論理積、排他的論理和などをとればよい。こうして、４列のデータすべてについて論理演算を行い、演算結果としてＹ１，Ｙ２，Ｙ３，Ｙ４を得る。続いて、これら演算結果と端末機１０から与えられた暗号データＸ１，Ｘ２，Ｘ３，Ｘ４との間で、それぞれ第７図に示すように所定の論理演算を行い、演算結果としてＺ１，Ｚ２，Ｚ３，Ｚ４を得る。これらを大きい順（または小さい順でもよい）に並べると、第８図に示すように、Ｚ３＞Ｚ４＞Ｚ１＞Ｚ２となったとする。これから、新たな順位データは「３４１２」と決定できる。このように、端末機１０からＩＣカード２０へ暗号データを与えることにより、セキュリティをより向上させることができる。特に、端末機１０とＩＣカード２０との間に何らかの回線が用いられている場合、この回線を介しての通信を盗聴された場合でも、順位データが漏洩することを防ぐことができる。

以上が暗号データのデコード手順の一例である。デコードが完了したら、ステップＳ１４において、順位データの書き替えが行われる。すなわち、順位データ領域２３に新たな順位データである「３４１２」が書き込まれる。そして、ステップＳ１５において、この書き替え作業が正常に行われたかが判断され、正常であればステップＳ１６で正常ステータスがセットされ、何らかの異常があればステップＳ１７においてエラーステータスがセットされる。

以上、３種類のコマンド処理の手順を説明したが、各コマンド処理が終了すると、ステップＳ１８において、全処理を終了するか否かが判断される。たとえば、全処理を終了すべきことを示す一般コマンドが与えられた場合には、ステップＳ１８を経て全手順が終了する。終了しない場合は、再びステップＳ２のコマンド入力に戻る。このとき、正常ステータスかエラーステーテスのいずれかがセットされているので、次のコマンド入力時に端末機１０側に何らかのメッセージを与えることができる。

なお、上述した実施例は本願発明の一実施態様を開示するものであり、本願発明はこの実施例のみに限定されるものではない。特に、暗号データのデコード方法は、これ以外にも種々の方法を適用することが可能である。また、ここでは１バイトの単位データを１桁のデータとして扱ったが、必ずしも１バイトを１桁とする必要はない。

〔発明の効果〕

(1)　本願第１の発明によれば、外部の端末機から優先順位の登録を更新することができるため、他人に照合手順を知られたとしても、優先順位を変えてしまえば、もはや他人の不正なアクセスを受けることがなく、セキュリティが向上する。また優先順位を変更する操作を行わない限り、同じ照合手順でアクセスできるため、操作性も良好である。

(2)　本願第２の発明によれば、優先順位の登録更新操作を行う場合、新たな優先順位を示す順

位データは、そのままではなく暗号データの形式で端末機からＩＣカードへと伝えられるため、セキュリティ性がより向上する。

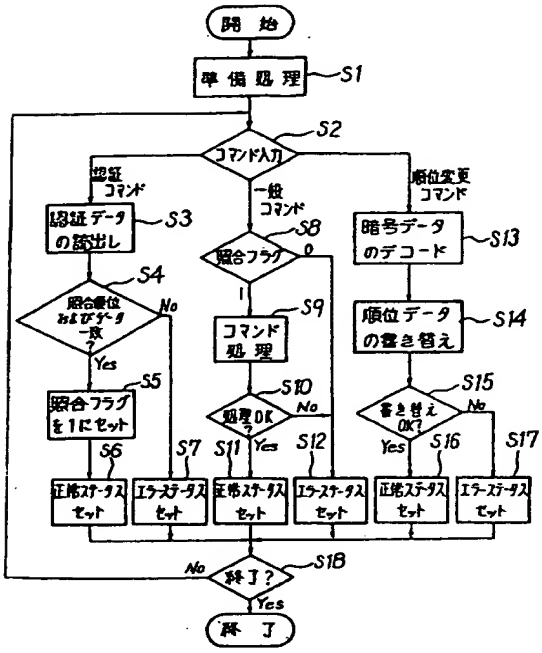
(3)　本願第３の発明によれば、ＩＣカード固有の識別データに基づいて生成された行列と、与えられた暗号データと、に基づいて優先順位が決定されるため、セキュリティ性の高い更新作業が可能になる。

４．図面の簡単な説明

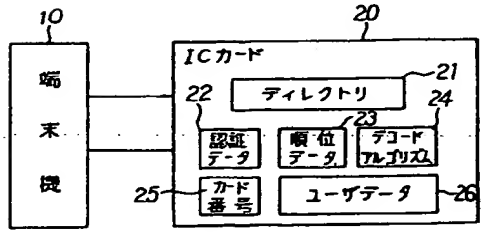
第１図は本発明の一実施例に係る認証方法を利用したＩＣカードのアクセス手順を示す流れ図、第２図は端末機１０にＩＣカード２０を接続した状態を示すブロック図、第３図は認証データの一例を示す図、第４図は順位データの一例を示す図、第５図はカード番号データの一例を示す図、第６図～第８図は本発明に係る暗号データのデコード手順に必要な論理演算を示す図である。

出願人代理人　志　村　　浩

特開平3-185586 (6)



第１図



第２図

22 認証データ領域

A6	87	B9	32	18	(認証データ①)
14	22	2A	6B	53	(認証データ②)
92	F8	EA	90	17	(認証データ③)
46	8D	5F	22	DB	(認証データ④)

第３図

23 順位データ領域

2	4	1	3

第４図

25 カード番号領域

A0	A1	A2	A3	A4	A5	A6	A7	A8
A9	AA	AB	AC	AD	AE	AF	B0	B1

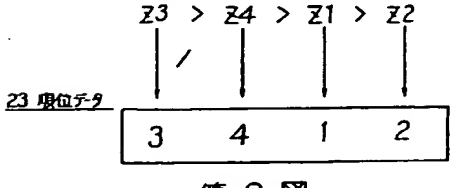
第５図

A0	A1	A2	A3
A4	A5	A6	A7
A8	A9	AA	AB
AC	AD	AE	AF
B0	B1	20	20
Y1	Y2	Y3	Y4

第６図

X1	X2	X3	X4
Y1	Y2	Y3	Y4
Z1	Z2	Z3	Z4

第７図



第８図